



REC'D 18 FEB 2003	
WIPO	PCT

**PRIORITY  
DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

**Aktenzeichen:** 101 64 495.7

**Anmeldetag:** 28. Dezember 2001

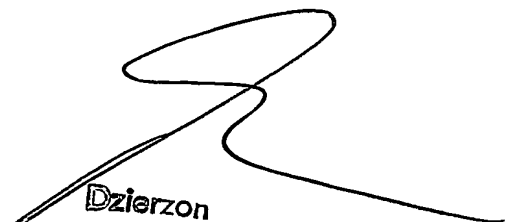
**Anmelder/Inhaber:** Siemens Aktiengesellschaft, München/DE

**Bezeichnung:** Fehlertolerantes Automatisierungssystem

**IPC:** G 05 B 9/02

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 7. August 2002  
**Deutsches Patent- und Markenamt**  
**Der Präsident**  
Im Auftrag

  
Dzierzon

## Beschreibung

## Fehlertolerantes Automatisierungssystem

5 Die Erfindung liegt auf dem Gebiet von Automatisierungssteuern  
rungen bzw. Automatisierungssystemen. Automatisierungssysteme  
werden insbesondere bei Produktionsmaschinen, Werkzeugmaschi-  
nen, Handhabungsautomaten, industriellen Prozessen und indus-  
triellen Fertigungen eingesetzt.

10

Automatisierungssysteme unterliegen verschiedensten Anforder-  
ungen, wie z.B. denen nach flexibler und/oder sicherer  
und/oder konsistenter Reaktion auf Ereignisse wie:

- 15 • Verarbeitungsfehler im Anwenderprogramm wie z.B. einer  
Division durch Null und/oder dem Verletzen von Array-  
grenzen
- Zugriffsfehler bei I/O Variablen - Input/Output Variab-  
len
- 20 • Zugriffsfehler beim Lesen und Schreiben von Systemvari-  
ablen

5

Diese Anforderungen gelten insbesondere für eine frei pro-  
grammierbare Automatisierungssystem. Weist die Automatisie-  
rungssteuerung bzw. ein Automatisierungssystem Multitasking-  
Eigenschaften auf so verschärfen sich die Anforderungen. Dies  
gilt beispielsweise für ein frei programmierbares Automati-  
sierungssystem für Produktionsmaschinen mit Multitasking-Ei-  
genschaften, das aufgrund integrierter Technologie- und Re-  
gelungsfunktionalität harten Echtzeiteigenschaften zu genügen  
30 hat.

35

In einer Automatisierungssteuerung bzw. in einem Automatisie-  
rungssystem wurden die obig beschriebenen Anforderungen ins-  
besondere dann, wenn Echtzeitanforderungen zu erfüllen sind  
bisher über synchrone Exceptions gelöst. Bei synchronen Ex-  
ceptions werden Anwenderprogramme unmittelbar mit der glei-

chen Priorität gestartet wie der bearbeitete Task, in dem ein Fehler aufgetreten ist.

Nachteilig bei dieser Lösung ist, dass die Lösung mit syn-  
5 chronen Exceptions in einem Automatisierungssystem bzw. in  
einer Automatisierungssteuerung mit hochprioren zyklischen  
Tasks nur bedingt einsetzbar ist, da die Gesamtlaufzeit der  
hochprioren zyklischen Taskebenen begrenzt ist.

10 Der Erfindung liegt die Aufgabe zugrunde, die Reaktion auf  
Fehler zu verbessern.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren zur  
Fehlerbehandlung bei einem Automatisierungssystem gelöst bei  
15 dem bei zumindest einem Verarbeitungsfehler und/oder zumin-  
dest einem Zugriffsfehler zumindest eine Fehlerreaktionsfunk-  
tionsfunktion ausgelöst wird, wobei die Fehlerreaktionsfunk-  
tion zumindest parametrierbar und/oder programmierbar ist.

20 Dies trifft insbesondere auf echtzeit Automatisierungssysteme  
zu. Durch Automatisierungssysteme sind verschiedenste Forde-  
rungen zu erfüllen. Dies sind beispielsweise flexible, si-  
chere und/oder konsistente Reaktionen auf:

- Verarbeitungsfehler im Anwenderprogramm, z.B. Division  
5 durch Null, Verletzen von Array-Grenzen,
- Zugriffsfehler bei I/O-Variable - Input/Output Variable,
- Zugriffsfehler beim Lesen und Schreiben von Systemvariab-  
len.

30 Diese Forderungen sind insbesondere bei einem frei program-  
mierbaren Automatisierungssystem zur Produktionsmaschine mit  
Multitasking-Eigenschaften, das aufgrund integrierter Techno-  
logie- und Regelungsfunktionalität harten Echtzeiteigenschaf-  
ten zu genügen hat, zu erfüllen. Bei Automatisierungssystemen  
35 ohne harte Echtzeit wurde bisher über synchrone Exceptions,  
welches Anwenderprogramme sind, die unmittelbar mit der glei-  
chen Priorität gestartet werden wie die bearbeitete

Task/Aufgabe, in der ein Fehler auftritt, gelöst. Erfindungsgemäß werden die oben beschriebenen Forderungen auch bei Echtzeit-Anforderungen erfüllt. Dies gilt insbesondere für ein Automatisierungssystem mit hochprioren zyklischen Tasks, wobei die Regelungsgüte gewährleistet bleibt. Hohe Anforderungen an Regelgüte und Dynamik eines Automatisierungssystems bleiben gewahrt. Die Forderung nach einer flexiblen, sicheren, konsistenten Reaktion auf Fehler ist durch einen durchgängigen konsistenten Gesamtansatz mittels der Definition / Realisierung von:

- Zugriffsfunktionen und/oder
  - eines definierten konfigurierbaren Ablaufverhaltens bei Zugriffsfehler bei Nichtanwendung der Zugriffsfunktion und/oder
  - eines definierten Verhaltens bei Auftreten von Verarbeitungsfehlern im Anwenderprogramm
- erfindungsgemäß ermöglicht.

Bei der Definition/Realisierung:

- von Zugriffsfunktionen
- sind Zugriffsfehler über parametrierbare Zugriffsfunktionen abfangbar, wobei in vorteilhafter Weise die Möglichkeit besteht, bei einem Fehler ein vordefiniertes Verhalten zu erzeugen, z.B. einen projektierten Ersatzwert zu nehmen, den letzten Wert weiter zu nehmen und/oder einen Grenzwert einzusetzen, und/oder;
- ist das Verhalten der Zugriffsfunktion über Parameter und damit unmittelbar am Aufruf einstellbar, und/oder;
- bedingt die Ausführung der Zugriffsfunktion auch bei einem Zugriffsfehler keinen Start der Fehlerbearbeitungs-Task, und/oder;
- ist die Zugriffsfunktion in jedem Tasktyp verwendbar;
- eines definierten kundenfigurierbaren Ablaufverhalten bei zumindest einem Zugriffsfehler bei Nichtanwendung der Zugriffsfunktionen bzw. der Zugriffsfunktion:

- ist vom System ein konfiguriertes Verhalten ausführbar, wenn Zugriffsfehler auftreten, ohne dass eine Zugriffsfunktion verwendet wird, z.B. Übernahme des Ersatzwertes, Übernahme des letzten Wertes, oder Start der Fehlerbearbeitungs-Task, in der die Reaktion flexibel ausprogrammiert werden kann;
  - ist ein definiertes einstellbares Verhalten bei Auftreten von Verarbeitungsfehlern im Anwenderprogramm erzielbar, wobei folgendes wählbar ist:
    - Start der Fehlerbearbeitungs-Task bei Verarbeitungsfehler im Anwenderprogramm;
    - oder direktes Überführen des Systems in den Stop-Zustand.
- Die Fehlerbearbeitungstask besitzt beispielsweise dabei zumindest eine der folgenden Eigenschaften:
- in der Fehlerbearbeitungs-Task kann ein Anwenderprogramm zur Reaktion auf den Verarbeitungsfehler oder Zugriffsfehler eingehängt werden;
  - der Fehlerbearbeitungstask wird in der Task-Startinformation mitgegeben, in welcher Task der Fehler aufgetreten ist und von welcher Art der Zugriffsfehler oder der Bearbeitungsfehler ist;
  - die Fehlerbearbeitungs-Task besitzt im Ablaufsystem eine definierte Priorität im Automatisierungssystem, die die hochprioritären zyklischen Tasks, z.B. von Motion Control, nicht behindert; diese Priorität ist dabei wahlweise fest oder einstellbar, jedoch unterhalb der Prioritätsstufe der hochprioritären zyklischen Tasks für Bewegungssteuerung und Regelung;
  - der Start der Fehlerbearbeitungs-Task führt zu Stop und Abbruch der Task, in deren Anwenderprogramm der Fehler aufgetreten ist;
  - nicht-zyklische Tasks können über Programmierung in dem Fehlerbearbeitungs-Task neu gestartet werden;
  - es wird damit ein konsistentes Systemver- und Ablaufverhalten auch in harten Echtzeitsystemen erreicht.

Durch die erfindungsgemäße Ausgestaltung eines Automatisierungssystems sind Zugriffsfehler direkt in flexible parametrierbare Zugriffsfunktionen abfangbar. Reaktionen auf Zugriffsziele und Verarbeitungsfehler sind in einer Task ausprogrammierbar, wobei die Task im Fehlerfall gestartet wird. Die erfindungsgemäße Fehlerbehandlung ist vorteilhafterweise verbunden mit dem Nichtabbruch oder der Nichtbeeinflussung hochpriorer zyklischer Systemtasks, wie sie z.B. bei Motion Control-Aufgaben auftreten. Derartige Aufgaben sind beispielsweise eine Interpolation und/oder eine Regelung.

Mit Hilfe der erfindungsgemäßen Fehlerbehandlung ist ein sicheres Systemverhalten des Automatisierungssystem erreichbar, wobei der Task beendbar ist, in welchem ein Fehler aufgetreten ist. In vorteilhafter Weise sind nicht-zyklische Tasks neu aufsetzbar. Beim Neuaufsetzen nicht-zyklischer Tasks werden entweder die Startwerte des ursprünglichen Tasks verwendet oder aber Zwischenergebnisse des abgebrochenen Tasks. Die erfindungsgemäße Fehlerbehandlung ist vorteilhafterweise verbunden mit dem Absteuern des Systems bei Auftreten von Fehlern in zyklischen Tasks, da in diesem Fall die wiederholte Abarbeitung und/oder der Abbruch der zyklischen Tasks nicht unbedingt sinnvoll ist. In vorteilhafter Weise wird erfindungsgemäß ein konsistentes Systemverhalten erreicht, auch dann, wenn das System nicht in Stop geht.

In einer vorteilhaften Weise wird erfindungsgemäß die Gesamtlaufzeit eines hochprioren zyklischen Tasks nicht überschritten um eine vereinbarte Regelungs- und/oder Steuerungsgüte zu gewährleisten. Dies gilt insbesondere bei Automatisierungssteuerungen und/oder Automatisierungssystemen, wobei diese Begriffe gleichbedeutend benutzbar sind, mit harten Echtzeitanforderungen.

Das erfindungsgemäße Automatisierungssystem ist vorteilhaft bei einer Produktionsmaschine und/oder einer Werkzeugmaschine eingesetzt.

- 5 Weitere vorteilhafte Ausführungen der Erfindung sind den Unteransprüchen 2 bis 10 entnehmbar.

Ein Ausführungsbeispiel ist in der Figuren 1 dargestellt. Dabei zeigt

10

Figur 1 Funktionen unterschiedlicher Prioritäten eines Automatisierungssystems

15

Die Darstellung gemäß Figur 1 zeigt verschieden Tasks, welche in einem Automatisierungssystem ablauffähig sind. Der Begriff Task ist dabei im Sinne des Begriffs Funktion anwendbar, wobei die Funktion zumindest eine Aufgabe beinhaltet. In der Figur sind die folgenden Tasks aufgeführt, wobei diese unterschiedliche Prioritäten aufweisen:

20

- Niederpriore zyklische und nichtzyklische Tasks
- Interrupt Tasks
- Hochpriore zyklische Tasks
- Hochpriore zyklische System Tasks

5

Die Tasks wurden mit steigender Priorität aufgelistet, wobei die Verwendung des Plurals keinen Hinweis darauf gibt, ob es sich um einen oder mehreren Tasks handelt.

30

Ein oder mehrere Fehlerbearbeitungstasks sind der Priorität nach Interrupt Tasks und/oder niederprioren zyklischen und/oder nichtzyklischen Tasks nebengestellt.

Bei folgenden Tasks:

35

- niederpriore zyklische Tasks
- niederpriore nichtzyklische Tasks

- interrupt Tasks
- hochpriore zyklische Tasks
- Fehlerbearbeitungstasks

5 sind Zugriffsfunktionen in allen Anwendertasks verwendbar.



## Patentansprüche

1. Verfahren zur Fehlerbehandlung bei einem echtzeit Automatisierungssystem bei dem durch zumindest einen Verarbeitungsfehler und/oder Zugriffsfehler zumindest eine Fehlerreaktionsfunktionsfunktion ausgelöst wird, wobei die Fehlerreaktionsfunktion parametrierbar und/oder programmierbar ist.
2. Verfahren nach Anspruch 1,  
dadurch gekennzeichnet, dass Zugriffsfehler mit Hilfe von parametrierbaren Zugriffsfunktionen abgefangen werden.
3. Verfahren nach Anspruch 1 oder 2,  
dadurch gekennzeichnet, dass eine Funktion programmierbar wird, welche als Reaktion auf Zugriffsfehler und/oder Verarbeitungsfehler gestartet wird.
4. Verfahren nach einem der vorgenannten Ansprüche 1 bis 3,  
dadurch gekennzeichnet, dass zumindest hochpriorre zyklische Systemfunktionen durch die Fehlerreaktionsfunktion unbeeinflusst ausgeführt werden.
5. Verfahren nach einem der vorgenannten Ansprüche 1 bis 4,  
dadurch gekennzeichnet, dass zumindest hochpriorre zyklische Systemfunktionen auch bei Ausführung einer Fehlerreaktionsfunktion abbruchslos weitergeführt werden.
6. Verfahren nach einem der vorgenannten Ansprüche 1 bis 5,  
dadurch gekennzeichnet, dass Funktionen, welche eine Fehlfunktion aufweisen abgebrochen werden, wobei ein sicheres Verhalten des Automatisierungssystems beibehalten wird.
7. Verfahren nach einem der vorgenannten Ansprüche 1 bis 6,

d a d u r c h g e k e n n z e i c h n e t , dass abgebrochene nichtzyklische Funktionen neu gestartet werden, wobei dabei auf die vorangegangene abgebrochene Funktion aufgesetzt wird.

5

8. Verfahren nach einem der vorgenannten Ansprüche 1 bis 6, d a d u r c h g e k e n n z e i c h n e t , dass bei Fehlern in zyklischen Funktionen das Automatisierungssystem abgesteuert wird.

10

9. Verfahren nach einem der vorgenannten Ansprüche 1 bis 8, d a d u r c h g e k e n n z e i c h n e t , dass beim Auftreten von Fehlern durch das Automatisierungssystem ein konsistentes Systemverhalten erzeugt wird ohne das Automatisierungssystem zu stoppen.

15

10. Verwendung des Verfahrens nach einem der vorgenannten Ansprüche, d a d u r c h g e k e n n z e i c h n e t , dass die Verwendung bei einer Werkzeugmaschine und/oder einer Produktionsmaschine erfolgt.

20

11. Vorrichtung zur Durchführung des Verfahrens nach einem der vorgenannten Ansprüche, d a d u r c h g e k e n n z e i c h n e t , dass die Vorrichtung ein Automatisierungssystem ist.

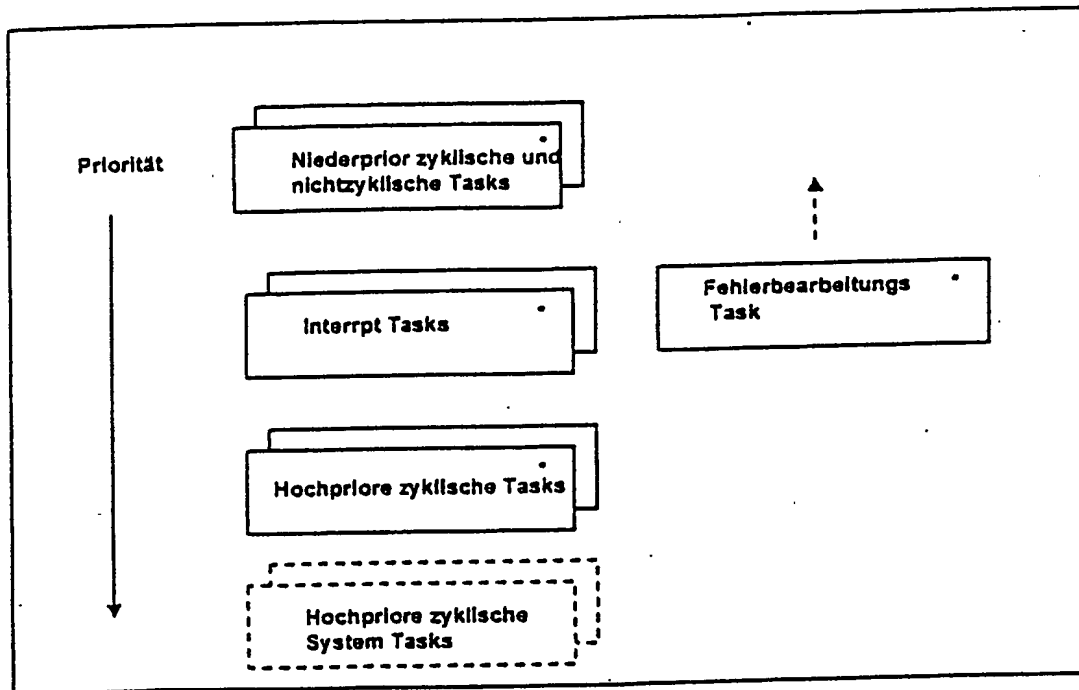
25

## Zusammenfassung

## Fehlertolerantes Automatisierungssystem

- 5 Die Erfindung betrifft ein Automatisierungssystem, bei welchem die Reaktion auf Fehler verbessert ist. Dies gelingt mit einem Verfahren zur Fehlerbehandlung bei einem echtzeit Automatisierungssystem bei dem durch zumindest einen Verarbeitungsfehler und/oder Zugriffsfehler zumindest eine Fehlerreaktionsfunktionsfunktion ausgelöst wird, wobei die Fehlerreaktionsfunktion parametrierbar und/oder programmierbar ist.
- 10

Fig 1



\*: Zugriffsfunktionen können in allen Anwendertasks verwendet werden;

Fig 1